Opinnäytetyö (AMK)

Tietojenkäsittely

2018

Tiia Summe

TODISTUSTAAKAN TÄYTTYMINEN YRITYKSISSÄ

– yleinen tietosuoja-asetus

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tietojenkäsittely

2018 | 36 sivua, 5 liitesivua

Tiia Summe

TODISTUSTAAKAN TÄYTTYMINEN YRITYKSISSÄ

- tietosuoja-asetus

GDPR (General Data Protection Regulation) on uusi EU:n yleinen tietosuoja-asetus, jonka soveltaminen tuo merkittäviä muutoksia tietosuojan sääntelyyn koko EU:n alueella. Tietosuoja-asetus asettaa organisaatioille osoitusvelvollisuuden, joka tarkoittaa, että organisaatioiden tulee pystyä osoittamaan asetuksen vaatimusten ja sen määrittämien tietosuojaperiaatteiden toteutuminen toiminnassaan. Tietosuoja-asetusta tarkasteltiin tässä opinnäytetyössä asetuksen vaatimusten täyttämisen osoittamisen osalta. Opinnäytetyön tavoitteena oli kuvata selkeillä kokonaisuuksilla niitä keinoja, joilla organisaatiot voivat tietosuoja-asetuksen vaatiman osoitusvelvollisuuden täyttää. Toteutettavat keinot oli tarkoitus huomioida niin organisatoriselta kuin tekniseltäkin näkökantilta.

Opinnäytetyön kokonaisuutta rakentaessa keskityttiin pääasiallisesti asetuksen määrittämien tietosuojaperiaatteiden tutkimiseen. Näiden tietosuojaperiaatteiden lisäksi opinnäytetyössä tutkittiin tietosuoja-asetuksen sisältämiä muita keskeisiä aiheita. Opinnäytetyön tutkimusmenetelmä oli kvalitatiivinen ja opinnäytetyön toteutuksessa hyödynnettiin tietosuoja-asetusta sekä sen perusteella toteutettuja aineistoja ja kirjallisuutta. Lisäksi toteutuksessa hyödynnettiin laajasti teknisen tietoturvan toteuttamiseen keskittyviä aineistoja, jotta pystyttiin myös tekniseltä tasolta kuvaamaan toimet, joita organisaatioiden tulisi tietosuojaperiaatteiden pohjalta toteuttaa.

Opinnäytetyön tavoitteissa onnistuttiin ja lopputuloksena on kattava yhteenveto siitä millaisilla teknisillä ja organisatorisilla toimilla organisaatiot voivat osoitusvelvollisuuden täyttää.

Johtopäätöksenä voidaan todeta, että varsinkin dokumentaation osalta vaihtoehtoja osoitusvelvollisuuden täyttämiseen on monia, joten jokainen organisaatio voi valita ne keinot, jotka parhaiten sopivat ja tukevat niiden omaa toimintaa.

ASIASANAT:

yleinen tietosuoja-asetus, GDPR, osoitusvelvollisuus, rekisteröity, rekisterinpitäjä, henkilötietojen käsittelijä

BACHELOR´S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Information technology

2018 | 36 pages, 5 appendices

Tiia Summe

FULFILLMENT OF THE BURDEN OF PROOF IN COMPANIES

- General Data Protection Regulation

The EU General Data Protection Regulation (GDPR) is a huge change in data privacy regulation. The aim of the GDPR is protect the rights of individuals and to give EU citizens ultimate control over their personal data. This thesis examines how the requirements defined by the GDPR are implemented. Burden of proof means that the new GDPR puts in place the “accountability principle” according to which every data controller is obliged to prove its fulfillment of legal requirements. The aim of the thesis was to comprehensively describe the mechanisms through which organizations can fulfill the burden of proof as defined by GDPR. The mechanisms to be implemented were to be taken into account both from the organizational and the technical point of view.

The focus of this thesis was mainly on examining the data protection principles defined by GDPR. In addition to these data protection principles, the thesis also examines other key issues in the GDPR. The methodology of the thesis was qualitative. The sources used in this thesis were the GDPR, GDPR-related literature as well as extensive materials focusing on the implementation of technical security.

The objectives of the Thesis were successful and the final result is a comprehensive summary of what technical and organizational measures organizations need in order to fulfill the burden of proof.

As a conclusion, there are many alternatives to fulfilling the burden of proof, so each organization can choose the mechanisms that best suit and support their own operations.

KEYWORDS:

GDPR, data privacy, burden of proof, accountability principle, data subject, data controller, data handler

SISÄLTÖ

SANASTO

Audit trail	Tapahtumaketju, jolla pystytään selvittämään tapahtumien kulku (Valtiovarainministeriö 2009, 26-27).
GDPR	General Data Protection Regulation on uusi EU:n yleinen tietosuoja-asetus (Hanninen ym. 2017, 11).
Henkilötieto	Kaikki tunnistettuun tai tunnistettavissa olevaan henkilöön liittyvä tieto (Hanninen ym. 2017, 19-20).
Henkilötietojen käsittely	Kaikki toiminnot, joita kohdistetaan henkilötietoihin joko manuaalisesti tai automaattista käsittelyä hyödyntäen (Hanninen ym. 2017, 20).
Henkilötietojen käsittelijä	Rekisterinpitäjän lukuun henkilötietoja käsittelevä taho (Hanninen ym. 2017, 22).
Lokitieto	Merkintä, joka on kerätty käyttäjäkohtaisesti järjestelmästä, jossa henkilötietoja käsitellään (Tietosuojavaltuutetun toimisto 2012).
Rekisterinpitäjä	Taho, joka päättää henkilötietojen keräämisestä ja niiden käyttötarkoituksista (Hanninen ym. 2017, 22).
Rekisteröity	Luonnollinen henkilö, jota henkilötiedot ja niiden käsittely koskevat (Hanninen ym. 2017, 20).
Riski	Tavoitteisiin vaikuttava mahdollinen negatiivinen lopputulos (Valtiovarainministeriö 2017b, 11).
Riskienhallinta	Organisaation toiminto, jolla ohjataan ja johdetaan riskejä (Valtiovarainministeriö 2017b, 11).
Suostumus	Vapaaehtoinen, yksilöity, yksiselitteinen ja tietoinen tahdonilmaisu, jolla rekisteröity hyväksyy henkilötietojensa käsittelyn (Hanninen ym. 2017, 23).
Tietosuoja	Luonnollisen henkilön yksityisyyttä turvaava perusoikeus (Tietosuojavaltuutetun toimisto 2013).

1 JOHDANTO

Tämä opinnäytetyö käsittelee tietosuoja-asetuksen rekisterinpitäjille asettamaa osoitusvelvollisuutta.

Valitsin aiheen opinnäytetyölle tietosuoja-asetuksen ajankohtaisuuden sekä siihen liittyvän suuren kiinnostukseni pohjalta. Lisäksi työskentelen tietoturvayrityksessä tietosuoja-asetuksen tuomien haasteiden parissa, joten työ tukee varmasti ammatillista kasvuani.

GDPR (General Data Protection Regulation) on uusi, koko EU:n laajuinen tietosuoja-asetus (2016/679), jonka soveltaminen alkaa 25.5.2018. Tietosuoja-asetuksen tarkoituksena on parantaa henkilötietojen suojaa ja rekisteröidyn oikeuksia sekä luoda Euroopan unionille vahva tietosuojakehys ja täten yhtenäistää henkilötietojen käsittelyn sääntely kaikissa EU/ETA-jäsenmaissa. (Tietosuojavaltuutetun toimisto 2015.)

Asetus tuo mukanaan tarkennuksia voimassa olevaan tietosuojan sääntelyyn (Suomessa henkilötietolaki 523/1999) sekä monia uusia velvoitteita. Tietosuojavelvoitteiden laiminlyönnistä tai rikkomisesta voidaan rekisterinpitäjille osoittaa merkittäviä sanktiomaksuja. (Tietosuojavaltuutetun toimisto 2015.)

Tietosuoja-asetus asettaa rekisterinpitäjille todistustaakan (Tietosuojavaltuutetun toimisto 2015). Opinnäytetyön tarkoituksena on kuvailla, mitä kaikkea yritysten tulee ottaa huomioon todistustaakan eli osoitusvelvollisuuden täyttymiseksi. Opinnäytetyössä myös kuvaillaan toimet, joilla yritykset voivat todistustaakan täyttymisen osoittaa. Tietosuoja-asetuksen mukaan tulevaisuudessa ei riitä, että rekisterinpitäjät kertovat pyrkivänsä noudattamaan asetuksen säännöksiä vaan niiden huomioiminen yrityksen toiminnassa tulee myös pystyä osoittamaan. Tietosuoja-asetus määrittää sen, mitä rekisterinpitäjän tulee voida osoittaa, mutta asetus ei kerro kaikkia niitä keinoja, miten ne voidaan osoittaa, joten opinnäytetyön tarkoituksena on kuvailla nämä keinot.

Opinnäyte kuvaa sen, miten henkilötietojen käsittelyn tietosuojaperiaatteet lainmukaisuus, kohtuullisuus, läpinäkyvyys ja käyttösidonnaisuus huomioidaan sekä miten tietojen minimointi, täsmällisyys, eheys & luottamuksellisuus sekä säilytysajan rajaaminen voidaan osoittaa.

Lisäksi opinnäytetyössä kuvataan yleisesti tietosuoja-asetusta, rekisterinpitäjän vastuita asetuksen noudattamisessa sekä rekisteröidyn oikeuksia. Tämän jälkeen on kuvattu toimet, joiden toteuttamisen avulla voidaan varmistua siitä, että rekisterinpitäjän toiminnassa voidaan todistaa tietosuoja-asetuksen osoitusvelvollisuuden täyttyminen.

Opinnäytetyön kirjoittamiseen on käytetty apuna tietosuoja-asetusta sekä tietosuojaa ja henkilötietojen käsittelyä koskevaa kirjallisuutta sekä verkkojulkaisuja.

2 TIETOSUOJA-ASETUKSEN TAUSTAA

Tässä luvussa kerrotaan yleisesti tietosuoja-asetuksesta, sen synnyn perusteista sekä sen mukanaan tuomista uudistuksista ja täsmennyksistä rekisteröidyn oikeuksiin ja rekisterinpitäjille osoitettuihin vaatimuksiin.

Yleinen tietosuoja-asetus eli kansainvälisesti tunnettu GDPR (Lyhenne englanninkielisestä nimestä General Data Protection Regulation) on 25.5.2018 alkaen suoraan sovellettavaa lainsäädäntöä koko EU:n alueella. (Hanninen, Laine, Rantala, Rusi & Varhela. 2017,13.) Asetus koskee tietosuojaa ja sitä, miten henkilötietojen käsittely turvataan ja säännöstely yhtenäistetään koko EU:n alueella. Asetus astui voimaan 24.5.2016 ja kahden vuoden siirtymäajan jälkeen toukokuussa 2018, yritysten henkilötietojen käsittelyn tulee olla tietosuoja-asetuksen vaatimusten mukaista. (Talus, Autio, Hänninen, Pihamaa & Kantonen. 2017, 9.)

EU:n tietosuojasäännöt uudistettiin, koska aiempi vuonna 1995 EU:ssa säädetty henkilötietodirektiivi on astunut voimaan digiajan ulkopuolella. Tuolloin ei ollut olemassa nykyisiä, lukuisia verkkopalveluita eikä niiden mukanaan tuomia tietosuojahaasteita. Asetuksen voimaantulolla halutaan vahvistaa ihmisten perusoikeuksia digitaaliajassa sekä varmistaa, että oikeus henkilötietojen suojaan voidaan taata myös tänä jatkuvasti kehittyvänä aikana. Asetuksen uusien sääntöjen myötä myös digitaalisen talouden kehittäminen helpottuu. (Tietosuojavaltuutetun toimisto 2016.)

2.1 Tietosuoja-asetuksen tarkoitus

Tietosuoja-asetuksen syntyyn on vaikuttanut tavoite tietosuojan sääntelyn yhtenäistämisestä ja ajantasaistamisesta. Ajan tasalla olevalla sääntelyllä voidaan vastata tietosuojaa koskeviin haasteisiin, jotka aiheutuvat globalisaatiosta sekä teknologian kehityksestä. Yhtenäisillä tietosuojaa koskevilla säännöksillä ja luottamuksen rakentamisella voidaan myös tukea digitaalitalouden kehittymistä sisämarkkinoilla. Lisäksi tietosuoja-asetus vahvistaa rekisteröidyn oikeuksia valvoa sitä, miten heidän henkilötietojaan käsitellään lisäämällä käsittelyn avoimuutta ja läpinäkyvyyttä. (Talus ym. 2017, 9.)

Tietosuoja-asetusta sovelletaan kaikkeen henkilötietojen käsittelyyn, niin julkisella kuin yksityiselläkin sektorilla yrityksen tai organisaation koosta riippumatta. Asetuksen soveltamiseen ei siis vaikuta esimerkiksi henkilötietojen käsittelyn laajuus tai käsiteltävien henkilötietojen luonne. (Talus ym. 2017, 9.)

2.2 Tietosuojaperiaatteet

Henkilötietojen käsittelyä koskevat tietosuojaperiaatteet on säädetty tietosuoja-asetuksessa. Henkilötietojen käsittelylle on jo aiemminkin ollut voimassa periaatteita, mutta tietosuoja-asetus tuo täsmennyksiä niille. (Hanninen ym. 2017, 47.) Nämä tietosuojaperiaatteet tulee ottaa huomioon kaikissa henkilötietojen käsittelyvaiheissa ja ne ohjaavat rekisterinpitäjää käsittelemään tietoja tavalla, joka kunnioittaa rekisteröidyn oikeuksia ja vapauksia. (Talus ym. 2017, 12.) Tietosuojaperiaatteiden osoittamiseksi rekisterinpitäjän

tulee toteuttaa asianmukaisia teknisiä ja organisatorisia toimenpiteitä (Hanninen ym. 2017, 55).

Tietosuojaperiaatteet, joiden käytännön toteutus tulee pystyä osoittamaan ovat:

- käsittelyn lainmukaisuus, kohtuullisuus ja läpinäkyvyys
- käyttötarkoitussidonnaisuus
- tietojen minimointi
- tietojen täsmällisyys
- tietojen säilytyksen rajoittaminen
- tietojen eheys ja luottamuksellisuus. (Hanninen ym. 2017, 48.)

2.3 Sisäänrakennettu ja oletusarvoinen tietosuoja

Sisäänrakennetun tietosuojan periaate tarkoittaa, että edellisessä luvussa mainitut henkilötietojen käsittelyä koskevat tietosuojaperiaatteet otetaan huomioon jo tuotteiden ja palveluiden suunnitteluvaiheissa. Yritysten tulisi tekniikan puolesta varmistaa, että ne pystyvät täyttämään tietosuojavelvoitteet jo ennen kuin ottavat käyttöön esimerkiksi henkilötietojen käsittelyyn liittyviä sovelluksia. Voidaan ajatella, että sitä tärkeämpää tietosuojan huomioiminen on suunnitteluvaiheessa, mitä korkeamman riskin käsittely rekisteröidyille aiheuttaa. (Hanninen ym. 2017, 54.)

Oletusarvoisen tietosuojan periaate puolestaan tarkoittaa, että tietoja käsiteltäessä henkilötietojen määrää pidetään oletusarvoisesti minimissään suhteessa tietojen käyttötarkoitukseen. Eli pääajatuksena on käsitellä vain kunkin käyttötarkoituksen kannalta tarpeellisia tietoja. Henkilötietojen käsittelyn laajuus, säilytysaika, määrä ja saatavilla olo ovat yksityiskohtia, jotka tulee ottaa tässä velvollisuudessa huomioon. (Talus ym. 2017, 13.) Esimerkiksi mobiilisovelluksissa oletusarvoinen tietosuoja otetaan huomioon siten, että asetukset, joilla yksityisyyden suojaa edistetään, ovat automaattisesti käytössä sovellusta käyttöön jo otettaessa (Hanninen ym. 2017, 54).

2.4 Henkilötietojen käsittelyn oikeusperusta

Tietosuoja-asetus vaatii, että kaikelle henkilötietojen käsittelylle tulee olla peruste (Talus ym. 2017, 19). Lain mukaista henkilötietojen käsittely voi asetuksen mukaan olla vain silloin, kun yksi tai useampi asetuksen määrittämä peruste täyttyy. Suostumus, sopimus sekä oikeutettu etu ovat yleisimpiä henkilötietojen käsittelyperusteita pienten ja keskisuurten yritysten keskuudessa. (Hanninen ym. 2017, 29.)

Asetuksen määrittämät lailliset henkilötietojen käsittelyn perusteet ovat seuraavat:

- rekisteröidyn antama suostumus
- sopimus, jonka osapuolena rekisteröity toimii
- lakisääteinen velvoite
- elintärkeä etu rekisteröidylle tai toiselle luonnolliselle henkilölle
- yleinen etu tai rekisterinpitäjän julkisen vallan käyttö

- Oikeutettu etu. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, 6 artikla.)

Suostumus

Suostumus on tahdonilmaisu, jossa rekisteröity antaa tietoisen ja yksiselitteisen, yksilöidyn ja vapaaehtoisen suostumuksena henkilötietojen käsittelyyn (Hanninen ym. 2017, 30). Esimerkki ihanteellisesta suostumuksen antamisesta on tilanne, jossa asiakas liittyy yrityksen kanta-asiakkaaksi verkkolomakkeen kautta. Ennen asiakkaan tietojen tallentamista järjestelmään, asiakkaalle avautuu lomakkeessa tietosuojaseloste, josta muun muassa henkilötietojen käsittelyn tarkoitukset voidaan tarkistaa. Hyväksyttyään selosteessa mainitut käsittelytoimet asiakas rastittaa suostumuksensa henkilötietojen käsittelyyn ja vasta tällöin tiedot tallentuvat järjestelmään.

Sopimus

Sopimusta voidaan käyttää henkilötietojen käsittelyn perusteena silloin, kun sopimuksen täyteen paneminen vaatii henkilötietojen käsittelyä (Hanninen ym. 2017, 30). Esimerkkejä sopimukseen perustuvasta henkilötietojen käsittelystä ovat lähes kaikki eri asiakkuuksiin liittyvät käsittelytoimet sekä myös työsopimuksen toteuttaminen työnantajan ja työntekijän välillä.

Lakisääteinen velvoite

Lakisääteinen velvoite henkilötietojen käsittelyn perusteena on silloin, kun rekisterinpitäjän on tarpeen toteuttaa henkilötietojen käsittelyä noudattaakseen lakisääteistä velvoitettaan (Hanninen ym. 2017, 31). Esimerkki lakisääteiseen velvoitteeseen perustuvasta henkilötietojen käsittelystä on veroviranomaisten toteuttama verotuksen toimittaminen.

Elintärkeä etu rekisteröidylle tai toiselle luonnolliselle henkilölle

Elintärkeä etu rekisteröidylle tai toiselle luonnolliselle henkilölle henkilötietojen käsittelyn perusteena toteutuu silloin, kun elintärkeä etu täytyy suojata (Hanninen ym. 2017, 31). Esimerkkejä näistä tapauksista voivat olla esimerkiksi luonnonkatastrofien ja ihmisten aiheuttamien katastrofien yhteydessä tapahtuva henkilötietojen käsittely informointitarkoituksissa.

Yleinen etu tai rekisterinpitäjän julkisen vallan käyttö

Yleinen etu tai rekisterinpitäjän julkisen vallan käyttö on henkilötietojen käsittelyn perusteena silloin, kun henkilötietojen käsittely on tarpeen julkisen tehtävän tai yleistä etua koskevan tehtävän suorittamiseksi (Hanninen ym. 2017, 31).

Oikeutettu etu

Oikeutettu etu henkilötietojen käsittelyn perusteena tarkoittaa sitä, että rekisteröidyn ja rekisterinpitäjän välillä on jokin asianmukainen suhde kuten työsuhde tai asiakkuus (Hanninen ym. 2017, 32).

2.5 Valvonta ja sanktiot

Tietosuoja-asetuksen vaatimusten toteutumista valvoo valvontaviranomainen. Tietosuoja-asetuksen soveltamisen valvonnan lisäksi valvontaviranomainen edistää tietoisuutta tietosuoja-asetuksesta sekä muun muassa ohjaa tietosuoja-asioissa. (Hanninen ym. 2017, 124.) Valvontaviranomainen on myös se taho, jolle tulee ilmoittaa ilman aiheetonta viivytystä henkilötietojen tietoturvaloukkauksista (Hanninen ym. 2017, 128).

Tietosuoja-asetus mahdollistaa valvontaviranomaisten määräämät merkittävät hallinnolliset sanktiot, mikäli tietosuoja-asetuksen vaatimuksia rikotaan. Sanktion määräämiseen ja määrään vaikuttavat monet asetuksessa määritetyt seikat, kuten esimerkiksi velvollisuus, jota on rikottu ja tapa, jolla asetuksen velvollisuuden rikkominen tuli valvontaviranomaisen tietoon. (Hanninen ym. 2017, 129.)

2.6 Tietosuojavastaava

Tietosuojavastaava on henkilö, joka valvoo henkilötietojen käsittelyä organisaatiossa ja varmistaa, että tietosuoja-asetuksen velvoitteita noudatetaan. Lisäksi tietosuojavastaava neuvoo tietosuoja-asetukseen liittyvissä kysymyksissä, osallistuu tietosuojan kehittämiseen organisaatiossa ja toimii yhteyshenkilönä niin rekisteröidyille kuin valvontaviranomaisillekin. (Hanninen ym. 2017, 122-123.)

Millä tahansa organisaatiolla on oikeus nimittää tietoturvavastaava, mutta tietosuoja-asetus kuitenkin edellyttää tietosuojavastaavan nimittämistä muutamassa tietyssä tilanteessa (Hanninen ym. 2017, 120-121).

Tilanteet, joissa tietoturvavastaava tulee nimittää ovat seuraavat:

- Yrityksen ydinliiketoimintaan kuuluu rekisteröityjen laajamittainen tai järjestelmällinen seuranta.
- Yrityksen ydinliiketoimintaan kuuluu rekisteröityjen, laajamittainen arkaluonteisten henkilötietojen käsittely. (Hanninen ym. 2017, 120–121.)
- Henkilötietoja käsittelevä organisaatio on julkishallinnon toimija (Tietosuojavaltuutetun toimisto 2017).

On tärkeää kuitenkin huomioida, että tietosuojavastaava ei ole vastuussa organisaation henkilötietojen käsittelyn lainmukaisuudesta eikä tietosuojavastaavan tehtävien hoitamisen kanssa saa olla eturistiriitoja, mikäli tietosuojavastaavalla on myös toinen tehtävä organisaatiossa (Tietosuojavaltuutetun toimisto 2017).

3 REKISTERINPITÄJÄN OSOITUSVELVOLLISUUS

Tässä luvussa kuvaillaan mitä tarkoittaa rekisterinpitäjän osoitusvelvollisuus ja mitä sen täyttämiseksi tulee ottaa huomioon. Myöhemmin, alkaen kappaleesta viisi opinnäytetyössä kuvataan niitä merkitseviä keinoja, joilla osoitusvelvollisuus voidaan täyttää.

Osoitusvelvollisuus on yksi tietosuoja-asetuksen tuomista keskeisimmistä muutoksista henkilötietojen käsittelyyn. Aiemmin henkilötietojen käsittelyä säännelleen henkilötietolain mukaan riitti, että säännöksiä noudatetaan, nyt tietosuoja-asetus velvoittaa rekisterinpitäjiltä kykyä osoittaa teknisin, hallinnollisin ja organisatorisin toimenpitein asetuksen vaatimusten noudattaminen henkilötietojen käsittelyssä. (Talus ym. 2017, 14; Hanninen ym. 2017, 51.)

Edellytyksenä osoitusvelvollisuuden toteuttamiseen on yrityksen tietosuojakysymyksiin suhtautuminen uudella näkökulmalla. Tietosuojaa koskevat kysymykset tulee esimerkiksi prosessien kannalta huomioida niin, että kaikki prosessit, joissa henkilötietoja käsitellään, ovat kattavasti dokumentoidut. Tietosuojakysymykset kattavat myös tietosuojaperiaatteiden käytännön toteutuksen ja tämä vaatii yrityksiltä lisäksi teknisiä- ja organisatorisia toimenpiteitä dokumentointeineen, jotta asetuksen osoitusvelvollisuus voidaan täyttää ja osoittaa. (Talus ym. 2017, 14.) Kattavan dokumentaation luomisella ja olemassa ololla sekä tietosuojaperiaatteiden huomioimisella organisaatio pystyy toteuttamaan kokonaiskuvan siitä, miten organisaatiossa henkilötietoja käsitellään ja miten tiedot on suojattu.

Täyttääkseen osoitusvelvollisuuden yrityksellä tulisi olla dokumentaatiota ainakin seuraavista asioista:

- henkilötietojen käyttötarkoitukset
- henkilötietojen käsittelytavat
- henkilötietojen käsittelyn perusteet
- käsiteltävät tietoryhmät
- tietosuojaorganisaation tai tietosuojavastaavan tiedot
- rekisteröidyn informoinnin keinot. (Hanninen ym. 2017, 52.)

4 REKISTERÖIDYN OIKEUKSIEN TOTEUTTAMINEN

Tässä luvussa kuvataan tietosuoja-asetuksen määrittämät rekisteröidyn oikeudet, jotka rekisterinpitäjän pitää pystyä toteuttamaan. Luvussa kuvataan myös tarkemmin jokaisen rekisteröidyn oikeuden tarkoitus.

Perusperiaatteena rekisteröidyn oikeuksille on henkilötietojen suojan takaaminen. Yksi rekisterinpitäjän tärkeimmistä velvollisuuksista onkin rekisteröidyn oikeuksien toteuttaminen. Tietosuoja-asetuksessa on määritetty rekisteröidyn oikeuksia, jotka ovat osin samoja kuin henkilötietolakiin on aikanaan säädetty. Asetus kuitenkin sisältää yksityiskohtaisempia täsmennyksiä olemassa oleviin oikeuksiin, sekä tuo mukanaan myös uusia oikeuksia rekisteröidyille. (Pietikäinen 2016a.) Asetuksen tuomien muutosten myötä rekisterinpitäjien on varmistuttava siitä, että kaikissa organisaation prosesseissa otetaan huomioon rekisteröidyn oikeudet. Lisäksi tietojärjestelmillä tulee olla mahdollisuus taipua toteuttamaan nämä rekisteröidyn oikeudet (Talus ym. 2017, 23).

Rekisteröidyn oikeuksien toteuttamista suunnitellessa tulee ottaa huomioon myös henkilötietojen käsittelyperusta, sillä nämä ovat yhteyksissä toisiinsa. Osa rekisteröidyn oikeuksista liittyy vain tiettyihin käsittelyperusteisiin, kuten esimerkiksi myöhemmin esiin tuleva rekisteröidyn vastustamisoikeus. Henkilötietojen käsittelytoimintoja suunniteltaessa rekisterinpitäjän on hyvä ensin selvittää henkilötietojen käsittelyperuste ja sitten tämän mukaan toteutettavaksi määrätyt rekisteröidyn oikeudet. (Talus ym. 2017, 23.)

4.1 Oikeus tietojen poistamiseen (”Oikeus tulla unohdetuksi”)

Rekisteröidyllä on olemassa rajoitettu oikeus saada yritys poistamaan häntä koskevat henkilötiedot (Hanninen ym. 2017. 62). Ne tilanteet, joissa rekisteröity voi tätä oikeuttaan käyttää on kuvattu seuraavaksi.

Rekisteröidyllä on oikeus saada yritys poistamaan häntä koskevat tiedot niissä tapauksissa, joissa yrityksellä ei ole tietojen säilyttämiseen muuta perustetta kuin rekisteröidyn antama suostumus ja rekisteröity haluaa peruttaa antamansa suostumuksen. Rekisteröidyllä on oikeus tulla unohdetuksi myös niissä tapauksissa, joissa henkilötietoja ei enää tarvita niihin tarkoituksiin, joihin ne on alun perin kerätty. Rekisteröidyn pyynnön perusteella tiedot tulee poistaa tapauksissa, joissa henkilötietoja on käsitelty lainvastaisesti tai kun rekisteröity on käyttänyt oikeuttaan vastustaa henkilötietojen käsittelyä ja käsittelyyn ei ole suoramarkkinoinnin lisäksi muuta perusteltua syytä. (Hanninen ym. 2017, 61–62.)

Lisäksi rekisteröidyllä on oikeus tulla unohdetuksi lainsäädäntöön perustuen silloin, kun yrityksen tulee noudattaa velvollisuuttaan poistaa tiedot. Myös lapsena internetiin saatetut tiedot on mahdollista poistaa, kun henkilötietoja on kerätty yhteiskunnan palveluja tarjottaessa alaikäiselle lapselle. (Hanninen ym. 2017, 62.)

Yrityksen tulee ilman aiheetonta viivytystä poistaa rekisteröidyn tiedot henkilörekistereistään, mikäli rekisteröidyllä on oikeus käyttää oikeuttaan tulla unohdetuksi. (Hanninen ym. 2017, 63.)

4.2 Oikeus tietojen oikaisemiseen

Rekisteröidyllä on oikeus vaatia tietojensa oikaisemista niissä tapauksissa, kun rekisteröityä koskevat tiedot ovat virheellisiä tai epätarkkoja. Käyttäessään oikeuttaan tietojen oikaisemiseen, on rekisteröidyllä mahdollisuus toimittaa rekisterinpitäjälle lisäselvityksiä täydentääkseen puutteellisia tietoja. Tietojen oikaisua ei voi kuitenkaan vaatia yrityksessä mahdollisesti oleviin, rekisteröityä koskeviin historiatietoihin. (Hanninen ym. 2017, 61.)

4.3 Oikeus saada pääsy tietoihin

Rekisteröidyllä on oikeus saada pääsy häntä koskeviin henkilötietoihin niissä tapauksissa, joissa yritys on rekisteröidyn pyynnöstä vahvistanut käsittelevänsä häntä koskevia henkilötietoja (Hanninen. 2017, 59). Tämä rekisteröidyn oikeus täsmentää aiemmin henkilötietolaissa säädettyä rekisteröidyn tarkastusoikeutta (Talus ym. 2017, 25).

Tiedot, joita rekisteröidyn on oikeus saada yritykseltä ovat seuraavat:

- henkilötietojen käsittelytarkoitukset
- käsiteltävät henkilötietoryhmät
- kaikki ne vastaanottajat sekä vastaanottajaryhmät, joille yritys on luovuttanut tai on luovuttamassa rekisteröidyn henkilötietoja
- henkilötiedon elinkaari ja mikäli elinkaarta ei voida ilmoittaa niin elinkaaren määrittelykriteerit
- henkilötietojen alkuperän tiedot
- tieto mahdollisesta automaattisesta päätöksenteosta ja siihen liittyvistä logiikasta ja käsittelyn merkittävyydestä sekä seurauksista rekisteröidylle. (Hanninen ym. 2017, 59-60.)

Rekisteröidyn oikeus päästä tietoihin kattaa myös seuraavat:

- oikeus tehdä valitus valvontaviranomaiselle
- oikeus pyytää yritystä poistamaan ja oikaisemaan tietoja, sekä
- oikeus rajoittaa ja vastustaa henkilötietojen käsittelyä. (Hanninen ym. 2017, 59–60.)

4.4 Oikeus vastustaa henkilötietojen käsittelyä ja automaattisesti tehtävät yksittäispäätökset

Rekisteröidyllä on oikeus vastustaa henkilötietojen käsittelyä tietosuoja-asetukseen sidotuissa, tietyissä tilanteissa (Talus ym. 2017, 27). Kuten kappaleen alussa kerrottiin, liittyy tämä rekisteröidyn oikeus vain osaan henkilötietojen käsittelyperusteista. Vastustamisoikeutta voidaan käyttää sellaisissa henkilötietojen käsittelytilanteissa, joissa käsittely perustuu tehtävän suorittamiseen, joka koskee yleistä etua, julkisen vallan käyttöön,

johon rekisterinpitäjä on oikeutettu tai oikeutetun edun toteuttamiseen kolmannelle osapuolelle. Näiden lisäksi vastustamisoikeutta voidaan käyttää suoramarkkinoinnin tarkoituksiin kohdistuvaan henkilötietojen käsittelyyn sekä historiallisiin, tilastollisiin ja tieteellisiin käsittelytarkoituksiin. Historiallista, tilastollista ja tieteellistä käsittelyä varten kohdistuvaa vastustamisoikeutta voidaan kuitenkin käyttää vain tietyin edellytyksin ja kansallisella lailla siihen voidaan säätää poikkeuksia. (Talus ym. 2017, 27.)

Mikäli rekisteröity käyttää vastustamisoikeuttaan on rekisterinpitäjällä velvollisuus lopettaa tietojen käsittely, ellei sillä ole mahdollisuutta osoittaa käsittelyn keskeyttämisen vaikuttavan negatiivisesti rekisteröidyn etuihin, oikeuksiin ja vapauksiin. Rekisterinpitäjä voi myös jatkaa käsittelyä silloin, kun se on tärkeää oikeudellisista syistä. (Hanninen ym. 2017, 67.)

Rekisteröidyllä on myös oikeus jäädä ulkopuolelle sellaisista päätöksentekotapauksista, jotka perustuvat pelkästään automaattiseen tietojen käsittelyyn tai tapauksissa, joilla voi olla häntä koskevia oikeusvaikutuksia (Hanninen ym. 2017, 69).

4.5 Oikeus käsittelyn rajoittamiseen

Rekisteröidyllä on oikeus saada tietojensa aktiivinen käsittely rajoitetuksi tietosuoja-asetuksessa määritetyissä neljässä eri tilanteessa. (Hanninen ym. 2017, 63-64).

Rekisterinpitäjän tulee rajoittaa henkilötietojen käsittelyä seuraavissa tapauksissa:

- Rekisteröity kiistää henkilötietojen paikkansapitävyyden.
- Henkilötiedoille suoritettu käsittely on lainvastaista ja rekisteröity vastustaa tietojen poistamista.
- Rekisteröidyn henkilötietoja ei enää tarvita rekisterinpitäjän käsittelytarkoituksiin, mutta rekisteröidyllä on tarve niihin oikeudellisia tarpeita varten.
- Tilanteessa, jossa rekisteröidyllä ja rekisterinpitäjällä on erimielisyys siitä saako rekisteröidyn henkilötietoja käsitellä rekisterinpitäjän perustein. (Hanninen ym. 2017, 64.)

Mikäli rekisteröidyllä on oikeus ja hän käyttää oikeuttaan vastustaa henkilötietojensa käsittelyä, yrityksellä on oikeus pitää tiedot tallennettuna, mutta niitä saa käsitellä vain kun:

- rekisteröity antaa käsittelyyn suostumuksen
- rekisterinpitäjällä on oikeudellisista syistä tarve käsitellä niitä, tai
- käsittelyllä suojataan toisen henkilön tai rekisterinpitäjän oikeuksia. (Hanninen ym. 2017, 46.)

4.6 Oikeus siirtää tiedot järjestelmästä toiseen

Rekisteröidyn tietojen käsittelemisen perusteena ollessa sopimus tai suostumus, tai mikäli tietojenkäsittelyä suoritetaan automaattisesti, on rekisteröidyllä oikeus saada tie-

tonsa siirrettyä suoraan rekisterinpitäjältä toiselle. Tietojen siirtäminen toiseen järjestelmään tulee voida tapahtua jäsennellyssä, yleisesti käytetyssä tai koneluettavassa muodossa. (Talus ym. 2017, 26.)

4.7 Oikeus saada läpinäkyvää informaatiota henkilötietojen käsittelystä

Henkilötietojen käsittelyn avoimuus on asia, jota tietosuoja-asetuksessa korostetaan. Asetus myös antaa henkilötietolakiin verraten tarkempia määräyksiä rekisteröidyn oikeuksien sekä informointivelvollisuuden käytäntöön tuomisesta. (Talus ym. 2017, 23.)

Rekisteröidyllä on oikeus saada henkilötietojen käsittelystä informaatiota selkeällä kielellä. Informaatiota henkilötietojen käsittelystä tulee olla saatavilla myös jo ennen tietojen käsittelyn aloittamista. Rekisteröidyllä on oikeus saada tietoa muun muassa siitä, miten tietoja kerätään ja mihin tarkoituksiin, missä määrin tietoja käsitellään tai tullaan myöhemmin käsittelemään. (Hanninen ym. 2017, 73.)

Rekisteröidyn pyytämien toimenpiteiden toteuttamiseen on rekisterinpitäjällä kuukauden määräaika. Tiettyjen edellytysten toteutuessa voidaan aikaa pitkittää. Rekisterinpitäjällä on myös kuukausi aikaa ilmoittaa rekisteröidylle siitä, miksi rekisteröidyn pyytämiä toimenpiteitä ei aiota toteuttaa. Tällöin rekisterinpitäjällä on kuitenkin velvollisuus informoida rekisteröityä tämän oikeussuojakeinoista, joista esimerkkinä on oikeus tehdä valitus tietosuojaviranomaiselle. Lisäksi rekisterinpitäjällä on kuukausi aikaa toimittaa rekisteröidylle tämän pyytämät tiedot henkilörekisterien sisällöstä koskien itseään. (Talus ym. 2017, 24.)

5 DOKUMENTAATION MERKITYS

Tässä luvussa kuvataan dokumentoinnin merkitystä osoitusvelvollisuuden täyttymisen kannalta. Tietosuoja-asetus velvoittaa dokumentoimaan tietosuojaperiaatteiden noudattamisen, mutta asetuksessa ei kuitenkaan tarkenneta kaikkea sitä, mitä nämä dokumentit voivat olla ja mitä niissä tulee ottaa huomioon. Luvussa selviää, että asetuksen vaatimia organisatorisia toimenpiteitä voivat olla esimerkiksi henkilöstölle osoitetut ohjeistukset ja määräykset sekä henkilötietoja käsittelevien prosessien dokumentointi.

Ajantasaisella ja kattavalla dokumentaatiolla voidaan osoittaa, että organisaatiossa tietosuojasta on huolehdittu (Valtiovarainministeriö 2016).

5.1 Henkilötietojen käsittelyn prosessidokumentaatio

Rekisterinpitäjän osoitusvelvollisuuden vuoksi yritysten tulee kuvata henkilötietojen käsittelyyn liittyvät prosessit. (Hanninen ym. 2017, 51).

Kun huomioidaan asetuksen määrittämät, jo aiemmin työssä mainitut tietosuojaperiaatteet niin käytännössä tämä olisi huomioitava siten, että kaikki henkilötietojen käsittelyä koskevat prosessit yrityksessä tulee tunnistaa, määrittää ja dokumentoida niin, että dokumentaatiosta selviää koko henkilötiedon elinkaari. Näin prosessidokumentaation avulla voidaan osoittaa, että käsittelyyn käytetään vain sen tarkoituksen kannalta tarpeellisia henkilötietoja sekä se, miten laajasti ja millaisen säilytysajan puitteissa tietoja käsitellään. Erilaisia organisaation prosesseja ovat esimerkiksi rekrytointiprosessi, henkilöstöhallinnan prosessit sekä identiteetinhallintaan liittyvät prosessit.

Tietosuojaperiaatteisiin pohjautuen, prosessidokumentaatiossa olisi tärkeää kuvata seuraavat asiat, jotta tietosuojaperiaatteet otetaan huomioon ja osoitusvelvollisuus näiltä osin täyttyy:

- henkilötietojen käsittelytoiminnon nimi, johon prosessi liittyy
- prosessissa käsiteltävät henkilötiedot
- prosessissa käsiteltävien henkilötietojen käsittelyperuste
- mistä käsiteltävät henkilötiedot saadaan
- prosessin aikana henkilötietojen käsittelyyn oikeutetut henkilöryhmät
- tieto henkilötietojen suojaamisesta prosessin aikana
- kuinka kauan kyseisessä prosessissa henkilötietoja tarvitaan
- henkilötietojen poistomenettely käsittelyn tarpeellisuuden päätyttyä

Tietosuoja-asetus vaatii, että henkilötietojen käsittelyyn annettu suostumus pitää pystyä rekisterinpitäjän toimesta osoittamaan (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, artikla 7). Prosessidokumentaatiota laatiessa on siis tärkeää ottaa huomioon se seikka, että mikäli henkilötietojen käsittelyperuste prosessissa on rekisteröidyn antama suostumus, tulisi myös tämä pystyä osoittamaan. Prosessidokumentaatioon olisi näissä tapauksissa hyvä selventää se, että miten suostumus on rekisteröidyltä pyydetty ja millä tavoin siitä on jäänyt osoitettava jälki.

5.2 Tietosuojariskienhallinnan dokumentaatio

Tietosuojan toteutumiseen organisaatiossa vaikuttaa hyvin toteutettu ja toimiva riskienhallinta (Valtiovarainministeriö 2017, 3). Riskienhallinta on koordinoitua toimintaa, jolla johdetaan, ohjataan ja hallitaan organisaation riskejä. Riskienhallintaan kuuluvat esimerkiksi organisaation johdon määrittämät toimintaohjeet ja riskienhallintaprosessi. (Valtiovarainministeriö 2017b, 11.)

Riskienhallintaprosessissa on useita vaiheita, jotka ovat toimintaympäristön määrittely, arviointiprosessi sekä tunnistettujen riskien käsittely. Jokaiseen tunnistettuun riskiin liittyy myös riskin katselmointi ja seuranta. Lisäksi merkittävässä osassa riskien käsittelyä ovat viestintä ja tiedonvaihto. (Valtiovarainministeriö 2017b, 18.)

Seuraavien alalukujen sisällöstä selviää, että organisaatiot ovat tietosuoja-asetuksen mukaan velvollisia arvioimaan oman toimintansa henkilötietojen käsittelyyn liittyviä riskejä, toteuttamaan hallintakeinoja riskien minimoimiseen sekä raportoimaan riskien toteutumisesta valvontaviranomaisille ja rekisteröidyille. Jotta riskiperusteinen lähestymistapa voidaan osoittaa ja ilmoitusvelvollisuuteen pystytään vastaamaan, voidaan johtopäätöksenä todeta, että organisaatiolla tulisi olla olemassa riskienhallinnan dokumentaatio, joka ottaa huomioon myös tietosuojariskit. Riskienhallintaprosessia määrittäessä on myös tärkeää määrittää riskienhallintaan liittyvät vastuut hallintatoimenpiteille ja varsinkin viestintään sekä tiedottamiseen, jotta esimerkiksi tietovuodosta kyetään ilmoittamaan 72 tunnin ilmoitusvelvollisuuden vaatimuksen mukaisesti.

Johdon määrittämien toimintaohjeiden voidaan ajatella olevan tärkeässä asemassa esimerkiksi siitä syystä, että jokainen organisaation alaisuudessa toimiva henkilö tietää miten toimia riskin havaitessaan. Tämä voidaan taas todeta eduksi siitä syystä, että tällöin riskiin pystyään reagoimaan mahdollisimman nopeasti ja tehokkaasti.

5.2.1 Riskiperusteinen lähestymistapa

Rekisterinpitäjän tulee määrittää organisaatiossa toteutettavat suojatoimet muun muassa sen mukaan, mikä on luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuva riski (Talus ym. 2017, 13).

Tietosuoja-asetus velvoittaa rekisterinpitäjältä riskiperusteista lähestymistapaa, jossa rekisterinpitäjän toteuttamat suojatoimet suhteutetaan siihen kuinka suuren riskin henkilötietojen käsittely aiheuttaa rekisteröidylle. Lähestymistavalla pyritään siihen, että tarvittavat suojatoimet pystytään suhteuttamaan riskien mukaisesti ja samalla voidaan poissulkea toiminnasta matalariskisten toiminteiden ylisääntelyä. Riskiperusteisen lähestymistavan noudattaminen vaatii organisaatiolta perusteellista arviota niistä riskeistä, jotka liittyvän sen henkilötietojen käsittelyyn. (Talus ym. 2017, 16.)

Riski on henkilötietojen käsittelyssä korkea esimerkiksi aina silloin kun käsitellään arkaluonteisia tietoja, lasten tietoja tai suuria määriä tietoja. Tästä syystä näiden tietojen käsittelyyn tulee kiinnittää erityisen tarkkaa huomiota (Hanninen ym. 2017, 26-27.)

Jotta organisaatio pystyy osoittamaan riskilähtöisen lähestymistavan toteutumisen toiminnassaan, tulee niillä siis olla mustaa valkoisella siitä, minkä perusteella suojauskeinoja on toteutettu ja riskejä arvioitu. Riskienarviointityökalun toteuttaminen on oleellisessa asemassa todistettavan arvioinnin suorittamiseksi. Tunnistettujen riskien perusteella on tehtävä arvio siitä, tuleeko henkilötietojen käsittelylle tehdä erillinen vaikutustenarviointi, jota käsitellään seuraavassa alaluvussa (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, artikla 35).

5.2.2 Tietosuojaa koskeva vaikutustenarviointi

Tietosuojan vaikutustenarviointi (Data Protection Impact Assesment, DPIA) on prosessi, jonka tarpeellisuus arvioidaan sen mukaan, kuinka suuren riskin henkilötietojen käsittelyn laajuus, luonne, asiayhteydet ja tarkoitukset aiheuttavat rekisteröidylle (Hanninen ym. 2017, 115).

Mikäli henkilötietojen käsittely aiheuttaa korkean riskin luonnollisen henkilön vapauksille ja oikeuksille, on rekisterinpitäjän suoritettava ennen käsittelyn aloittamista kyseinen vaikutustenarviointi, jonka avulla voidaan selvittää käsittelytoimien vaikutukset rekisteröidyille (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, artikla 35). Vaikutustenarvioinnin toteuttaminen on pakollista esimerkiksi silloin, kun arkaluontoisia henkilötietoja käsitellään laajamittaisesti, eli niitä käsitellään paljon ja pitkäaikaisesti (Hanninen ym. 2017, 116). Mikäli organisaatioon on nimitetty tietosuojavastaava, on rekisterinpitäjällä velvollisuus pyytää tältä neuvoja vaikutustenarviointia tehdessä (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, artikla 35).

Vaikutustenarvioinnissa selvitetään henkilötietojen käsittelyn tarpeellisuutta sekä sitä, miten tietosuoja on otettu huomioon kyseisessä käsittelytapahtumassa (Hanninen yms. 2017, 115). Lisäksi vaikutustenarvioinnissa tarkastellaan henkilötietojen käsittelyyn suunniteltuja toimenpiteitä sekä suojatoimia, joilla riskejä pystytään madaltamaan ja henkilötietojen suoja voidaan varmistaa. Vaikutustenarvioinnin tekemisellä voidaan edesauttaa osoitusvelvollisuuden toteutumista, joten sen suorittaminen on suositeltavaa, vaikka käsittelytoimet eivät aiheuttaisikaan rekisteröidylle merkittävää riskiä. (Talus ym. 2017, 17.)

Edeltävän tekstin perusteella voidaan siis todeta, että vaikutustenarvioinnilla tekemisellä on mahdollisuus löytää huomattavia epäkohtia tietosuojan suhteen yrityksen sisältä ja tämän perusteella miettiä jatkotoimet tietosuoja-asetuksen vaatimusten täyttämiseksi rekisterinpitäjän toiminnassa. Kokonaisuudessaan vaikutustenarvioinnilla on siis mahdollisuus saada hyvä ja tarkka kokonaiskuva organisaation prosesseista, palveluista sekä järjestelmistä. Tästä syystä vaikutustenarvioinnin toteuttaminen on myös hyvä dokumentaation luomisen ja osoitusvelvollisuuden täyttämisen apuväline kaikissa henkilötietoja käsittelevissä toiminnoissa, vaikka vaikutustenarvioinnin toteuttaminen ei olisikaan pakollista.

5.2.3 Poikkeamien dokumentoiminen ja ilmoitusvelvollisuus

Tietoturvallisuuden kannalta poikkeama tarkoittaa sellaista tahallista tai tahatonta tapahtumaa, jonka seurauksena tietojen tai palvelun luottamuksellisuus, eheys tai käytettävyys vaarantuu tai saattaa vaarantua (Valtiovarainministeriö 2017a, 12). Tämän luvun yhteydessä poikkeamalla tarkoitetaan tietoturvaloukkausta.

Tietosuoja-asetus tuo mukanaan uudistuksen, jonka seurauksena rekisterinpitäjällä on velvollisuus ilmoittaa tietosuojaviranomaiselle ja rekisteröidyille henkilötietojen tietoturvaloukkauksista ilman aiheetonta viivytystä 72 tunnin kuluessa loukkauksen ilmitulosta (Talus ym. 2017, 32).

Henkilötietojen tietoturvaloukkaus on tilanne, jossa henkilötiedot vahingossa, laittomasti tai oikeudettoman pääsyn seurauksena tuhoutuvat, häviävät tai muuttuvat. Henkilötietojen tietoturvaloukkaus on myös yhtä lailla tilanne, jossa henkilötietoja luvattomasti luovutetaan eteenpäin. (Hanninen ym. 2017, 108.)

Ilmoitusta tietosuojaviranomaiselle ei kuitenkaan tarvitse tehdä, kun voidaan varmistua, että tietoturvaloukkaus ei aiheuta riskiä rekisteröidyn oikeuksille ja vapauksille. Kaikista tietoturvaloukkauksista ei tarvitse myöskään ilmoittaa rekisteröidyille. Tapaukset, joissa ilmoitus tulee tehdä välittömästi, ovat ne henkilötietojen tietoturvaloukkaukset, joissa luonnollisten henkilöiden oikeuksille ja vapauksille todennäköisesti aiheutuu suuri riski. (Hanninen ym. 2017, 111.) Esimerkki tällaisesta tietoturvaloukkauksesta voi olla tilanne, jossa luonnollisten henkilöiden henkilötunnuksia tai luottokorttitietoja on joutunut tietoturvaloukkauksen kohteeksi.

Kaikki henkilötietoihin kohdistuneet tai niitä koskettaneet tietoturvaloukkaukset tulee kuitenkin dokumentoida myöhempää tarkastelua varten, sillä valvontaviranomainen voi dokumentaation avulla tarkastaa, että ilmoitusvelvollisuutta on noudatettu (Talus ym. 2017, 32).

Kaikista henkilötietojen käsittelyyn liittyvistä tietoturvaloukkauksista tulisi dokumentoida seuraavat tiedot:

- tietoturvaloukkauksen luonne
- vuodon kohteena olevan tiedon määrä ja luonne
- vaikutukset rekisteröidyille
- toteutetut korjaavat toimet jatkovahinkojen estämiseksi (Hanninen ym. 2017, 111.)

Jotta ilmoitusvelvollisuuteen pystytään vastaamaan, tulisi osana henkilötietojen käsittelyä luoda toimintatavat tietoturvaloukkausten varalle. Toimintatapojen tulisi sisältää ne tiedot, miten tietoturvaloukkaus tunnistetaan, miten niistä ilmoitetaan, miten ne ratkaistaan ja millä tavoin niistä luodaan tarpeellinen dokumentaatio. Dokumentoidulla toimintatavalla kyetään tehokkaasti minimoimaan vahinkoja ja palauttamaan toimintakyky. Lisäksi henkilöstön osaamisesta toimia tulisi huolehtia kriisitilanteiden varalle. (Talus ym. 2017, 33.)

5.3 Selosteet

Henkilötietolaki 1999/523 pitää sisällään vaatimuksen henkilötietorekistereistä laadittavista rekisteriselosteista (Henkilötietolaki 22.4.1999/523,10.§). Tietosuoja-asetuksessa ei ole kuitenkaan määritelty kuvaavia nimiä mahdollisille selostemuotoisille dokumenteille.

Tietosuoja-asetus vaatii rekisterinpitäjiltä ja henkilötietojen käsittelijöiltä kirjallisen dokumentaation ylläpitoa niistä henkilötietojen käsittelytoimista, jotka ovat kunkin vastuulla. Kyseinen käsittelytoimien dokumentaatio voidaan tietosuojaviranomaisten taholta pyytää esitettäväksi ja sen avulla voidaan osoittaa, että käsittelytoimet ovat tietosuoja-asetuksen mukaisia. (Talus ym. 2017, 14.) Asetuksessa kuitenkin mainitaan myös, että kyseinen vaatimus ei koske alle 250 työntekijän organisaatioita, ellei organisaation toiminta täytä asetuksessa mainittuja erityisehtoja, joiden mukaan vaatimus tulee toteuttaa myös vähemmän työntekijöitä työllistävissä organisaatioissa (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, artikla 30).

Erityisehdot ovat kuitenkin vielä tulkinnanvaraisia, koska ennakkotapauksia ei ole eikä tarkempia ohjeistuksia ole saatavilla. Tästä syystä rekisterinpitäjien tulee itse tulkita, koskeeko kyseinen vaatimus heitä.

Huomioon tulee kuitenkin ottaa, kuten opinnäytetyön luvusta ”rekisteröidyn oikeuksien toteuttaminen” käy ilmi, että kaikilla rekisterinpitäjillä on velvoite antaa rekisteröidyille läpinäkyvää informointia henkilötietojen käsittelystä ja rekisteröidyn oikeuksista. Tästä syystä edellä mainitun henkilötietojen käsittelyn toimien kuvaaminen on välttämätöntä kaikissa organisaatioissa, joissa henkilötietoja käsitellään niiden laajuudesta huolimatta.

Jotta rekisteröidyn oikeus saada läpinäkyvästi informaatiota toteutuu, olisi henkilötietojen käsittelystä oltava laadittu dokumentaatio, joka sisältää henkilötietojen käsittelyn periaatteet, vastuut ja rekisteröidyn oikeudet. Käytännössä dokumentaation tulisi olla helposti ymmärrettävä, helposti saatavilla oleva, selkeälukuinen ja tiivis, jotta rekisteröidyn oikeus toteutuu ja toteutuminen voidaan myös osoittaa.

Tällainen dokumentaatio muistuttaa hyvin pitkälti henkilötietolain vaatimaa rekisteriselostetta, joka on täydennetty informaatiolla rekisteröidyn oikeuksista (Tietosuojavaltuutetun toimisto 2014a). Tällaisesta rekisteriselostetta tarkemmasta selostemuotoisesta dokumentista käytetään nimeä tietosuojaseloste (Hanninen ym. 2017, 75).

Kaikkien rekisterinpitäjien ja henkilötietojen käsittelijöiden tulisi siis pitää esimerkiksi verkkosivuillaan esillä tietosuojaselostetta, jossa organisaation henkilötietojen käsittely kuvataan esimerkiksi seuraavan, tietosuoja-asetuksen vaatimuksiin pohjautuvan rungon mukaan:

- rekisterinpitäjän nimi
- yhteystiedot rekisteriä koskevissa asioissa
- rekisterin nimi
- henkilötietojen käsittelyn tarkoitus ja peruste
- rekisterin tietosisältö
- henkilötietojen säilytysaika
- säännönmukaiset tietolähteet

- tietojen säännönmukaiset luovutukset ja tietojen siirto Euroopan unionin tai Euroopan talousalueen ulkopuolelle
- rekisterin suojauksen periaatteet
- henkilötietojen käsittelyyn liittyvät rekisteröidyn oikeudet
- yhteydenotot rekisteriin liittyvissä asioissa
- tietosuojaselosteen muuttaminen

Tämän hetken tulkinnan mukaan hyvä keino toteuttaa osoitusvelvollisuus informointivelvollisuuden osalta on käydä läpi kaikki yrityksen henkilötietojen käsittelyyn liittyvät toimet ja jakaa tiedot sopiviin kokonaisuuksiin erillisiin tietosuojaselosteisiin. Tietosuojaselostekokonaisuuksia voivat olla esimerkiksi asiakas- ja markkinointirekisterit, työntekijä- ja yhteistyökumppanirekisterit sekä rekrytointiin liittyvät rekisterit.

5.4 Politiikat

Asianmukaisen tietosuojadokumentaation luominen on osa osoitusvelvollisuuden täyttymistä (Valtiovarainministeriö 2016).

Tietoturvapolitiikka on yksi osa organisaatioiden tietosuojadokumentaatiota, jolla on tavoite suojata ja turvata yrityksen tietoja. Tietoturvapolitiikka on dokumentti, jonka organisaation ylin johto hyväksyy ja johon on kuvattu yrityksen toimintatavat tietoturvallisuuden toteuttamisessa. Tietoturvapolitiikka sisältää organisaation tietoturvan toteutumista tukevat käytännöt sekä määräykset ja ohjeet, joita yrityksen toiminnassa tulee noudattaa. Sen sisältöön olisi hyvä liittää tieto erilaisista tietoturvavastuista, kuten tiedottamisen vastuista tietoturvaloukkaustilanteissa. (Koivunen 2011.) Kattava tietoturvapolitiikka siis ohjaa tietoturvallisuuden toteutumista organisaatiossa ja sillä pystytään osoittamaan yrityksen toimintatavat.

Tietosuojapolitiikka voi olla oma erillinen politiikkansa tai se voidaan sisällyttää osaksi organisaation tietoturvapolitiikkaa. Tietosuojapolitiikka kuvaa tietosuojan merkityksen organisaatiolle ja organisaation periaatteet henkilötietojen käsittelylle. Organisaatiossa kaiken henkilötietojen käsittelyn tulee nojautua tietosuojapolitiikkaan sekä voimassa olevaan lainsäädäntöön. (Valtiovarainministeriö 2016.) Tietosuojapolitiikka olisi hyvä tarkastaa ja päivätä vuosittain sekä aina, kun organisaatiossa tapahtuu muutoksia henkilötietojen käsittelyssä.

5.5 Ohjeistukset

Tietosuojaperiaatteiden toteutuminen vaatii organisaatioilta organisatorisia toimenpiteitä. Organisatorisia toimenpiteitä ovat esimerkiksi henkilöstölle osoitetut ohjeistukset, määräykset ja koulutukset (Talus ym. 2017, 13). Tietosuoja-asetus myös suoraan velvoittaa järjestämään henkilötietoja käsitteleville henkilöille tietosuojakoulutuksia (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, artikla 47). Voidaan todeta, että ilman henkilöstölle osoitettuja ohjeistuksia tai heille järjestettyjä tietosuojakoulutuksia, ei henkilöstön tietoisuutta yrityksen tietosuojakäytännöistä voida osoittaa. Asianmukaisilla ohjeistuksilla voidaan varmistua siitä, että henkilöstö tietää, miten henkilötietoja kuuluu

käsitellä oikein tietosuoja-asetuksen määrittämällä tavalla ja mitkä ovat käsittelijöiden käsittelyvastuut. Ainoastaan kirjallisten ohjeistusten olemassaolo ei välttämättä kuitenkaan itsessään täytä osoitusvelvollisuutta. Jotta organisaatioissa voidaan varmistua henkilöstön tietoisuudesta henkilötietojen käsittelyn ja siihen liittyvien velvollisuuksien suhteen, olisi henkilöstöltä hyvä jäädä merkintä ohjeistusten lukemisesta. Tämä voidaan toteuttaa yksikertaisuudessaan keräämällä henkilöstöltä allekirjoitettu kuittaus jo olemassa oleviin ohjeistuksiin sekä aina, kun uusi ohjeistus on julkaistu. Suuremmissa yrityksissä tehokas keino voi olla esimerkiksi yrityksen intranetiin toteutettu koulutusportaali, jossa ohjeistusten sisäistäminen varmistetaan kokeella, jonka suorituksesta jää sähköinen merkintä.

5.6 Tietotilinpäätös

Tietotilinpäätös on yksi organisaatioiden keinoista raportoida toimintaansa. Tietotilinpäätöksessä keskitytään raportoimaan organisaation tietoturvallisuutta, tietosuojaperiaatteisiin vastaamista sekä erilaisia tietovarantoja. (Tietosuojavaltuutetun toimisto 2014b.)

Kuten tähän menneessä työssä on käynyt ilmi, tietosuoja-asetus vaatii organisaatioilta perusteellista dokumentointia tietojenkäsittelytoimista. Tästä syystä on tietotilinpäätös kattava keino täyttää osoitusvelvollisuus näiltä osin.

Tietotilinpäätöksellä voidaan kuvata tietojenkäsittelyn nykytila organisaatiossa, sekä saadaan arvio tietoturvan ja tietosuojan toteutumisesta.

Tietoja, joita kattavan tilinpäätöksen tulisi sisältää ovat:

- organisaation hallussa olevat tietovarannot
- organisaation tietoarkkitehtuuri
- käsiteltävien tietojen laatu ja käytettävyys
- henkilötietojen käsittelyn periaatteet ja menettelytavat
- henkilötietojen suojauskeinot
- tietojen käytönvalvonta
- rekisteröidyn oikeuksien toteuttamiskeinot. (Tietosuojavaltuutetun toimisto 2014b.)

5.7 Sopimukset ulkoisien palveluntarjoajien kanssa

Moni organisaatio ulkoistaa palvelujaan toisille toimijoille ja usein tämä tarkoittaa myös henkilötietojen luovuttamista rekisterinpitäjän omien järjestelmien ulkopuolelle. Henkilötietojen käsittelyn voidaan siis ajatella toteutuvan monen eri organisaation kanssa yhteistyössä. Rekisterinpitäjien tulee kuitenkin huomioida, että vaikka tekemisen voi ulkoistaa niin vastuuta ei voi. Tästä syystä rekisterinpitäjällä on velvollisuus varmistaa, että henkilötietoja käsitellään tietosuoja-asetuksen vaatimalla tavalla myös ulkoisten palveluntarjoajien toimesta.

Kaikissa niissä tapauksissa, joissa toinen organisaatio käsittelee henkilötietoja rekisterinpitäjän puolesta tai lukuun, tulee näiden organisaatioiden välille tietosuoja-asetuksen

mukaan solmia tietosuojaa koskeva sopimus tai muu asiakirja. Tällaisissa tapauksissa muodostuu henkilötietoja vastaanottavasta organisaatiosta tietosuoja-asetuksen mukainen henkilötietojen käsittelijä. Rekisterinpitäjän ja henkilötietojen käsittelijän välinen tietosuojaa koskeva asiakirja voi olla täysin oma sopimuksensa tai esimerkiksi erillinen tietosuojaliite, joka liitetään organisaatioiden väliseen palvelusopimukseen. (Hanninen ym. 2017, 82.) Organisaatioiden välisen, tietosuojaa koskevan sopimuksen tarkoituksena on, että henkilötietojen käsittelijän varmistetaan toimivan tietosuoja-asetuksen vaatimalla tavalla (Talus ym. 2017, 22). Lisäksi sopimuksella on tärkeää osoittaa molempien osapuolten vastuut ja velvollisuudet (Hanninen ym. 2018, 82).

Organisaatioiden välisen tietosuojasopimuksen tulee sisältää seuraavat tiedot:

- kesto ja kohde henkilötietojen käsittelylle
- henkilötietojen käsittelyn tarkoitus ja luonne
- mitä käsiteltävät henkilötiedot ovat
- ne rekisteröityjen ryhmät, joita henkilötietojen käsittely koskee. (Hanninen ym. 2017, 83)

Tietosuoja-asetus määrittää suoraan seikkoja, joita organisaatioiden välisissä sopimuksissa tulee olla. Niitä ovat:

- henkilötietojen käsittely rekisterinpitäjän ohjeiden mukaisesti
- salassapitovelvollisuudet
- käsittelyn turvallisuudesta huolehtiminen henkilötietojen käsittelijän toiminnassa
- ehdot alihankkijoiden käyttämiselle henkilötietojen käsittelijän toiminnassa
- rekisteröityjen pyyntöihin vastaaminen
- henkilötietojen käsittelijän avustusvelvollisuus
- tietojen poistaminen tai palauttaminen rekisterinpitäjälle käsittelyn päätyttyä
- tarkastukset ja auditointioikeus. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679,28 artikla.)

5.8 Sertifioinnit

Yhtenä keinona osoittaa tietosuoja-asetuksen asettamien velvollisuuksien noudattaminen on tietosuojaa koskevien sertifiointimekanismien, tietosuojasinettien tai -merkkien käyttö (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, artikla 42).

Sertifioinnin voi myöntää akkreditoidut sertifiointielimet, jotka täyttävät tietosuoja-asetuksen vaatimukset ja joilla on tarpeellinen asiantuntemus tietosuojasta (Hanninen ym. 2017, 114). Sertifioinnilla saavutetaan rekisteröidyn mahdollisuus arvioida tietosuojan tasoa organisaation palveluiden ja tuotteiden osalta (Talus ym. 2017,14).

Tulee kuitenkin huomioida, että myönnetty sertifiointi, tietosuojasinetti tai -merkki ei vaikuta asetuksen noudattamisen velvollisuuksiin ja se voidaan perua, jos vaatimukset eivät enää organisaation kohdalla täyty. Lisäksi sertifiointi on voimassa kerrallaan kolme vuotta, jonka jälkeen se voidaan myöntää uudestaan, mikäli vaatimukset yhä täyttyvät. (Hanninen ym. 2017, 114.)

6 TEKNINEN TIETOTURVA JA TODISTUSTAAKKA

Tässä luvussa kuvaillaan teknisiä toimenpiteitä, jotka tulee ottaa huomioon ja toteuttaa, jotta voidaan vastata tietosuoja-asetuksen vaatimuksiin tietosuojaperiaatteiden toteuttamisesta ja näiltä osin vastata osoitusvelvollisuuteen.

Tietosuoja-asetus velvoittaa yritystä toteuttamaan tarvittavat tekniset toimenpiteet osoittaakseen asetuksen noudattaminen henkilötietojen käsittelyssä. Henkilötietojen asianmukainen turvallisuustaso on myös varmistettava tietojenkäsittelyn riskeihin ja henkilötietojen luonteeseen suhtautettuna huomioimalla uusin tekniikka ja toteuttamiskustannukset. (Hanninen ym. 2017, 106.)

6.1 Tietoturvallisuuden toteuttaminen

Organisaatioilla on velvollisuus varmistaa käsittelyn turvallisuus henkilötietoja käsitellessään. Turvallisuusvaatimukset kohdistuvat henkilötietojen eheyteen, luottamuksellisuuteen, käytettävyyteen sekä vikasietoisuuteen. (Hanninen ym. 2017, 107.) Tietosuoja-asetus vaatii, että henkilötiedot tulee suojata oikeudettomalta sekä vahingossa tapahtuvalta tietojen muuttumiselta, tuhoamiselta, luovuttamiselta tai pääsyltä tietojen siirron, käsittelyn tai säilytyksen aikana (Valtiovarainministeriö 2016, 24).

Henkilötietojen luottamuksellisuudella tarkoitetaan sitä, että henkilötietoihin tulee olla pääsy vain niillä henkilöillä, joilla on niiden käsittelyyn oikeus. Hieman tarkemmin avattuna tämä tarkoittaa, että organisaation sisällä käyttöoikeudet tulee rajata niin, että vain henkilöillä, joilla on työnsä puolesta oikeus käsitellä tietoja, pääsevät niihin käsiksi. Luonnollisesti henkilötiedot tulee suojata myös niin, ettei ulkopuolisilla, oikeudettomilla henkilöillä ole pääsyä tietoihin. (Hanninen ym. 2017, 107.) Pääsyn rajaaminen sekä käyttöoikeuksien hallinta tulee siis olla organisaatiossa kunnossa. Lisäksi luottamuksellisuutta organisaation toiminnassa voidaan ylläpitää huomioimalla tietojen salaus, vahvojen salasanakäytäntöjen toteutus, turvallinen tietoaineistojen hävitys sekä esimerkiksi metatietojen poistaminen tiedostoja käsitellessä (Hanninen ym. 2017, 107).

Tietojen eheyden eli oikeellisuuden varmistaminen taas perustuu pitkälti aiemmin mainittuun tietojen luottamuksellisuuteen. Kaiken henkilötiedon käsittelyn aikana tietojen muuttumattomuus tulee turvata. Tähän vaikuttaa paljon esimerkiksi juuri mainitun oikeudettoman pääsyn varmistaminen. (Hanninen ym. 2017, 107.)

Tietojen käytettävyyden takaaminen puolestaan tarkoittaa, että henkilötietojen käsittelyyn oikeutetuilla henkilöillä tulee olla pääsy tietoihin aina tarvittaessa. Lisäksi tiedot pitää pystyä palauttamaan mahdollisimman pian epäsuotuisan tilanteen, kuten teknisen vian tai esimerkiksi fyysisen uhkan tapahduttua. Toiminnan jatkuvuus pitää pystyä siis takaamaan, joten henkilötietojen varmuuskopioinneista huolehtiminen on suuressa osassa tietojen käytettävyyden toteuttamisessa. (Hanninen ym. 2017, 107.) Osaksi toteutusta pitäisi tuoda luvussa viisi mainittu riskienhallintaprosessi, jotta ei-toivotuista tilanteista pystytään toipumaan nopeasti ja tietojen käytettävyys pystytään palauttamaan mahdollisimman pian.

Vikasietoisuus puolestaan tarkoitetaan sitä, että organisaatiossa tulee olla teknisesti sellaiset tallennusratkaisut, jotka pystyvät mahdollisen häiriön kohdatessa, jatkamaan toimintaansa. Samalla järjestelmän tulisi pystyä toipumaan mahdollisimman pitkälle itse, kuitenkin niin, että voidaan varmistua, että häiriöstä selvitään ilman lisävahinkoja. (Hanninen ym. 2017, 107.)

6.2 Kyky poikkeamien havainnointiin

Luvussa viisi käsiteltiin poikkeamanhallinnan ja ilmoitusvelvollisuuden dokumentaatiota, josta selvisi, että rekisterinpitäjällä on 72 tunnin ilmoitusvelvollisuus henkilötietoihin kohdistuneista tietoturvaloukkauksista. Jotta organisaatiot pystyvät vastaamaan tähän ilmoitusvelvollisuuteen on niillä oltava kyky havaita poikkeamat. Havainnointikyky alkaa järjestelmä- sekä työasemaympäristöjen kattavalla dokumentaatiolla ja valvonnan suunnittelulla. (Valtiovarainministeriö 2016, 26.)

Rekisterinpitäjä voi huolehtia valvonnasta itse, mutta tällöin tulee huomioida, että se vaatii organisaatiolta resursseja sekä henkilökunnalta osaamista tiedostaa, millaisia poikkeamatilanteita tulee tunnistaa. Jotta kyvykkyys poikkeamienhallintaan voidaan osoittaa, vaatii toiminta kattavaa prosessimäärittelyä, johon on selkeästi kuvattu prosessissa toimivien henkilöiden roolit ja vastuut. (Valtiovarainministeriö 2016, 26-27.)

Tehokas keino valvoa ympäristöjä ja parantaa yrityksen tietoturvaa on tietoturvatapahtumien havainnointiohjelmisto eli SIEM-järjestelmä (Security Information and Event Management). (Valtiovarainministeriö 2016, 26.) Ympäristön tapahtumien havainnointi ja niiden jatkokäsittely sekä tietojen prosessointi ja syötteen tallentaminen ovat SIEM-ratkaisujen päätehtäviä. Tyypillisesti SIEM- ratkaisujen havainnointikyky perustuu verkkoliikenteen tapahtumista sekä lokitiedoista kerättyyn tietoon. Tuotetarjonta SIEM-ratkaisuille markkinoilla on laaja ja tarvittava kokonaisuus palvelulle on usein hyvin rakennettavissa kunkin organisaation tarpeiden mukaan. Jokaisessa tapauksessa SIEM-ratkaisu kuitenkin parantaa organisaatiossa ongelmien havainnointi- ja reagointikykyä sekä ohjaa henkilöresursseja kustannustehokkaiksi. (Vesamäki 2016.) Ulkoista palveluntarjoajaa poikkeamien havainnointiin käytettäessä tulee huomioida ilmoitusvelvollisuuteen liittyvät vastuut organisaatioiden välisessä sopimuksessa (Valtiovarainministeriö 2016, 27).

6.3 Lokienhallinta

Lokienhallinta on usein osana edellisessä alaluvussa mainittuja SIEM-ratkaisuja. Lokitieto on tallenne, joka on kerätty aikajärjestyksessä tapahtumasta (Viestintävirasto 2016, 2).

Lokienhallinta on merkittävä osa organisaation tietoturvallisuuden toteuttamista, sillä lokien keräämisellä voidaan varmistaa tietosuojan toteutuminen ja valvonta. Lokitiedot ovat välttämättömiä, jotta pystytään varmistamaan järjestelmien eheys ja muodostamaan luotettavia tapahtumaketjuja (audit trail) dokumentoimalla datan polkuja. Täten lokitiedolla pystyään esimerkiksi tietomurtotapahtumassa osoittamaan se mitä on tapahtunut, kuka teki ja mitä. (Valtiovarainministeriö 2009, 14.) Lokitietoja käytetään myös nor-

maalitilanteissa häiriöttömyyden ylläpitoon ja tilastoinnin tarkoituksiin (Valtiovarainministeriö 2009, 13). Lokiympäristö on hyvä silloin, kun se on eroteltu pois lokitettavasta järjestelmästä erilliseen lokiympäristöön, pääsynhallinta on vain tarpeelliselle käytölle rajattua ja lokien muuttaminen on estettyä (Viestintävirasto 2016, 2-4).

Koska lokit ovat niin sanotusti todisteita tapahtumista, tulee huomioida, että osoitusvelvollisuus täyttyy lokienhallinnan osalta vasta, kun lokien keräys on teknisesti suojattu ja lokitietojen eheys, laatu ja saatavuus on varmistettu.

Esimerkkinä voidaan ajatella järjestelmään kohdistunutta tietomurtotilannetta, jossa lokienhallinta on paikallista eli loki sijaitsee samassa ympäristössä kuin itse lokitettava järjestelmä. Tällaisessa tapauksessa paikallinen lokienhallinta tuo riskin todistustaakkaan, koska järjestelmään murtautuneella on myös mahdollisuus pyyhkiä tai muokata paikallisesti säilytettäviä lokitietoja. Tämän seurauksena lokitiedot eivät ole enää luotettavia eli niiden eheys on rikottu, koska niiden oikeellisuudesta ei voida varmistua. Tämän vuoksi paikallinen lokienhallinta ei ole suositeltavaa. Jotta lokien oikeellisuudesta voidaan varmistua kaikissa tilanteissa, kaikki oikeudet lokitietojen poistoon ja muokkaukseen on teknisesti estettävä myös järjestelmien ylläpitäjiltä (Viestintävirasto 2016, 4).

Hyvin toteutettuna suunnitelmallisella ja keskitetyllä lokienhallinnalla voidaan varmistaa se, mitä verkkoliikenteessä, järjestelmissä ja esimerkiksi kulunvalvonnassa tapahtuu. Lokienhallinta mahdollistaa tapahtumien jäljitettävyyden, kyvyn havaita poikkeamat sekä sen, että tapahtumien osapuolet ovat varmistettavissa. (Viestintävirasto 2016, 2-4.) Tästä syystä lokienhallinnalla voidaan tietosuojaperiaatteista osoittaa tietojen eheys ja luottamuksellisuus.

Lokien keräämisessä tulee kuitenkin ottaa huomioon tietosuojaperiaatteet, koska myös lokitiedot voivat muodostaa henkilörekisterin. Rekisteröityjen, käyttäjien ja ylläpitäjien tietosuoja tulee varmistaa, joten henkilötiedot tulee tunnistaa ja niiden säilömisen tarpeellisuus arvioida. (Viestintävirasto 2016, 6.) Tietosuoja-asetus säätelee lokien keräämistä siis samalla tavalla kuin muutakin henkilötietojen käsittelyä. Mikäli loki sisältää henkilötietoja henkilörekistereistä vaadittava rekisteriseloste voidaan lokien osalta laatia niin, että seloste on koko järjestelmästä ja siihen huomioidaan erikseen lokitiedot. Tietosuoja-asetuksen näkökulmasta tulisi myös miettiä sitä, että sisältääkö itse loki sellaista tietoa, joka tulisi lokittaa.

Merkinnät, joita lokiin tulisi vähintään sisällyttää ovat seuraavat:

- aikaleima tapahtumasta
- mitä tapahtumassa tehtiin tai yritettiin tehdä
- kuka tai mikä teki
- millä valtuuksilla tai oikeuksilla tapahtuma tehtiin
- mistä tapahtuma tehtiin tai mistä muutostieto on peräisin
- mihin resurssiin muutos kohdistui
- onnistuiko vai epäonnistuiko tapahtuma (Viestintävirasto 2016, 4.)

Tietoja joiden tallentamista lokiin tulee välttää ovat seuraavat:

- henkilötunnukset
- arkaluonteiset henkilötiedot
- luottokorttitiedot
- salasanat

- järjestelmien käyttöavaimet
- valtuutustiedot
- henkilöiden väliset viestiliikenteet (Viestintävirasto 2016, 5.)

6.4 Identiteetin- ja pääsynhallinnan toteutus

Yksinkertaisesti identiteetin- ja pääsynhallinta (IAM, Identity and Access Management) kertoo sen, kenellä on oikeus, mihin, miksi ja miten (Opitietosuojaa.fi 2015). Tietosuoja-asetus vaatii kykyä taata järjestelmien jatkuva luottamuksellisuus ja eheys (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, artikla 32).

Luvun ensimmäisessä alaluvussa käy ilmi, että henkilötietoihin pääsyn tulee olla hallittua ja rajattua, jotta juurikin tietojen luottamuksellisuus ja eheys voidaan taata. Tästä syystä voidaan todeta, että organisaatiolla tulisi olla teknisesti rajattu pääsynhallinta ja siihen liittyvää dokumentaatiota identiteetinhallinnasta ja pääsyoikeuksien myöntämisprosessista.

Identiteetin- ja pääsynhallinnan toteutus on laaja kokonaisuus. Seuraavassa on otettu kantaa toteutukseen siltä osin, miten toteutus on tärkeää huomioida tietosuoja-asetuksen vaatimusten näkökannalta.

Identiteetin- ja pääsynhallinnassa on tärkeää varmistaa, että käyttäjä voidaan tunnistaa ja käyttäjätunnukset, joilla henkilötietoja sisältäviä järjestelmiä käytetään, ovat aina henkilökohtaisia. Henkilökohtaisten käyttäjätunnusten avulla voidaan käyttäjän tekemät toimet liittää luotettavasti yksittäiseen henkilöön. Toteutus vaatii kuitenkin myös järjestelmäkohtaisen käyttäjärekisterin olemassaoloa, jossa myös käyttäjien tietoja pidetään ajan tasalla. Käyttöoikeudet järjestelmiin tulisi rajata niin, että käyttöoikeus tiettyyn toimintoon toteutetaan vain silloin, kun työtehtävän suorittaminen niin vaatii. Työtehtävien tai työroolin muuttuessa käyttöoikeudet on myös katselmoitava ja tarvittaessa päivitettävä. Käyttöoikeus on myös pystyttävä päättämään välittömästi, kun työtehtävä tai työrooli ei enää edellytä kyseisten tietojen käsittelyä. (Opitietosuojaa.fi 2015.)

Identiteetin- ja pääsynhallinnan toteutuksen ohella sen dokumentaatioon tulisi sisällyttää vastuut sisältävä prosessi käyttöoikeuksien myöntämisestä ja käyttöoikeuksien muutostarpeista, aina käyttöoikeuksien sulkemiseen saakka. Dokumentaatiossa tulisi ilmetä myös käyttöoikeuksien myöntöperusteet ja työroolit, joissa henkilötietoja on oikeus käsitellä. (Opitietosuojaa.fi 2015.)

Näillä dokumentaatiotoimilla voidaan siis osoittaa millä perustein pääsyoikeudet myönnetään ja että, henkilötietoihin pääsee käsiksi vain ne henkilöt, joilla on niihin työtehtäviensä perusteella edellytys. Näin ollaan aina ajan tasalla siitä, kellä on tietoihin pääsy ja millä oikeuksilla.

6.5 Järjestelmien toiminta

Tietosuoja-asetus velvoittaa, että tietosuojaperiaatteet sekä rekisteröidyn oikeuksien toteuttaminen tulee ottaa huomioon kaikessa henkilötietojen käsittelyssä organisaation sisällä. Asetukset vaatimuksien toteutuminen tulee siis varmistaa ja huomioida myös organisaation järjestelmä- ja sovelluskehityksessä sekä tulevissa järjestelmähankkeissa. (Valtiovarainministeriö 2016, 43.)

Opinnäytetyössäkin tähän mennessä esille tulleet asiat, jotka järjestelmissä ja sovelluksissa tulee ottaa huomioon, jotta osoitusvelvollisuus täyttyy ovat:

- tietojen poiston mahdollisuus
- käyttäjän suostumuksen pyytäminen ja tästä jäävä merkintä
- tiedon siirrettävyyden mahdollisuus toiseen järjestelmään
- tiedon käsittelyn rajoittamisen mahdollisuus
- tiedon kerääminen järjestelmästä koneluettavassa muodossa

Järjestelmien tulee pystyä taipumaan toteuttamaan rekisteröidyn oikeudet ja näistä tulee olla dokumentaatiota. Esimerkiksi automaattista tietojen poistoa tukevien järjestelmien dokumentaatiolla pystytään osoittamaan tiedon elinkaaren toteutuminen ja tietojen poistomahdollisuus rekisteröidyn käyttäessä oikeuksiaan.

6.6 Turva-arkkitehtuuri

Tähän menneessä esiin tulleista asioista voidaan päätellä, että tietoturvallisuuden toteutumiseen vaikuttavat monet eri osa-alueet.

Tietosuoja-asetus velvoittaa rekisterinpitäjää huolehtimaan tiedon turvaamisesta koko henkilötiedon elinkaaren ajan, kaikissa tiedon käsittelyvaiheissa. Henkilötiedot tulee näin ollen suojata myös tietojen säilytyksen ja siirron aikana.

Turvallinen verkko- ja järjestelmäarkkitehtuuri on yksi niistä osa-alueista, joka tulee tietojen käsittelyssä huomioida. Tämä osa-alue pitää sisällään esimerkiksi asianmukaiset palomuurit sekä salaukset, jotka kohdistuvat tietojen siirtoväyliin. (Valtiovarainministeriö 2016, 24-25.)

Seuraavassa on kuvattu mitä turvallisessa verkko- ja järjestelmäarkkitehtuurissa tulisi ottaa huomioon, jotta tietojen turvallisuus voidaan taata.

Palomuurit

Palomuuri on ohjelmisto tai laite, jonka tarkoituksena on hallita verkosta toiseen kulkevaa tietoliikennettä tai tietoliikennettä, joka kulkee verkon ja yksittäisen järjestelmän välillä (Suomen Automaatioseura ry 2010, 11). Palomuurin avulla voidaan estää muu kuin tarvittava ja erikseen sallittu liikenne (Suomen Automaatioseura ry 2010, 81). Tietojen luottamuksellisuus ja eheys voi vaarantua, mikäli palomuuri mahdollistaa kaiken liikenteen (Valtiovarainministeriö 2010, 43).

Palomuurin lisäksi voidaan verkossa käyttää hyökkäysten havaitsemiseen (IDS) tarkoitettuja laitteita tai ohjelmistoja. Nämä ohjelmistot kykenevät havaitsemaan verkossa tapahtuvia hyökkäyksiä. IPS eli hyökkäyksen estojärjestelmiä taas käytetään estämään verkossa havaittuja hyökkäyksiä. (Valtiovarainministeriö 2010, 83).

Myös palomuurilaitteiden lokitiedot tulee siirtää esimerkiksi erilliseen turvattuun lokipalvelimeen, jotta palomuurin lokitietoja ei pystytä ulkopuolisen toimesta muuttamaan tai lukemaan itse järjestelmästä (Valtiovarainministeriö 2009, 84-85). Kun palomuurin lokitiedot ovat luotettavia voidaan niiden avulla varmistaa esimerkiksi se mistä liikenne on tullut ja mihin se mennyt (Valtiovarainministeriö 2009, 36).

Tietosuojan kannalta voidaan todeta, että kyseiset ohjelmistot ja järjestelmät ovat tärkeitä tietojen luottamuksellisuuden ja eheyden toteutumiseksi.

Verkkojen eriyttäminen

Verkon eriyttämisellä tarkoitetaan sitä, että organisaation verkot ja niiden osat, jaotellaan toisistaan niin fyysisesti kuin loogistestikin käyttötarkoituksen mukaan. Erilaisia käyttötarkoituksia verkoille ovat esimerkiksi sisäverkko, hallintaverkko, testiverkko ja vierailijaverkko. Erilaiset käyttötarkoitukset luonnollisesti määrittävät verkon käyttäjäkunnan sekä suojauksen pohjavaatimukset, jotka ovat käyttötarpeissa erilaiset. (Valtiovarainministeriö 2010, 34).

Esimerkiksi organisaatiossa käytössä oleva vierailijaverkko tulee eriyttää muusta sisäverkosta. Vierailijaverkolla tulisi olla myös yhteys vain internettiin. (Valtiovarainministeriö 2010, 57). Verkon eriyttämisellä pystytään vaikuttamaan positiivisesti tietoturvaan, sillä haavoittuvaisuusriski on pienempi (Valtiovarainministeriö 2010, 34).

Voidaan siis todeta, että eriyttämisellä tietoa suojataan tehokkaasti, koska esimerkiksi haittaohjelmatartunta saadaan eristettyä vain tiettyyn verkon osaan, eikä se verkkojen eriyttämisen vuoksi pysty leviämään vapaasti.

Palvelinten kovennukset

Palvelinten koventaminen tarkoittaa turhan toiminnallisuuden poistamista, joita ei järjestelmien toiminnassa tarvita. Sillä voidaan tarkoittaa myös muutoksien tekemistä konfiguraatioihin, jolloin tietyn toiminnallisuuden poistaminen rajoittaa myös mahdollisuutta väärinkäyttöihin. (Suomen Automaatioseura ry 2010, 73.) Palvelinten koventaminen on siis toimiva keino tietoturvan parantamiseen sekä sisäisiä ja ulkoisia uhkia vastaan.

Siirtoväylien salaus

SSH- tai HTTPS-protokollien käyttöönoton avulla voidaan salata hallinta- ja valvontayhteyksissä kulkeva liikenne. Tällöin liikenteen tarkkaileminen tai muuttaminen on ulkopuolisen toimesta mahdotonta. Salaamattomia protokollia käyttäessä tulee tiedon salauksesta huolehtia muulla tavoin, kuten esimerkiksi VPN-yhteydellä. (Valtiovarainministeriö 2010, 83.) Jotta tiedonsiirto on turvallista, on siirtoväylien salaaminen tärkeä osa tietoturvallista verkkoa. Salauksen käyttäminen lisää tietoturvallisuutta merkittävästi ja edistää näin ollen tietosuoja-asetuksen vaatimusta tiedon luottamuksellisuudesta.

Opinnäytetyössä on tullut useasti selville, että dokumentoinnilla on suuri osuus osoitusvelvollisuuteen, sillä tietosuojaperiaatteiden toteutuminen tulee osoittaa. Siksi myös

turva-arkkitehtuurista on ylläpidettävä dokumentaatiota, jolla osoittaa miksi ja miten tietoturvallisuutta on toteutettu.

Edellä mainittujen tietoturvallisuuteen perustuvien toimien perusteella dokumentaatiota tulisi olla olemassa esimerkiksi seuraavista:

- palomuurilaitteissa sallittu liikenne
- palomuurilaitteissa tapahtuvan liikenteen dokumentointi
- verkkojen eriyttämistä havainnollistava kuva, jotta tiedostetaan missä verkkolaitteet sijaitsevat ja mitä lähiverkkoa alueissa on
- palvelinten kovennusten osalta tarpeellisiksi jätetyt toiminnallisuudet ja näiden osalta oikeudet muutosten tekemiseen
- siirtoväylien salaamisen osalta valittujen palvelujen seuranta ja toimintaohjeet haavoittuvaisuuksien löytämisen varalle

6.7 Organisaation fyysinen turvallisuus

Myös organisaation fyysisestä turvallisuudesta tulee huolehtia. Organisaation tilat, joissa henkilötietoja käsitellään tulisi rajata pääsykontrollein ja -rajauksin. Lisäksi laitteiden huoltotoimenpiteisiin tulisi sopia yhteiset, dokumentoidut käytännöt, jotta tietoa ei päädy kolmansille osapuolille. Sama asia koskee tapauksia, joissa laitteita vaihdetaan uusiin ja tämän seurauksena hävitetään tai luovutetaan eteenpäin. (Valtiovarainministeriö 2016, 25.)

6.8 Tietoturvatestaus

Luvussa kaksi kerrottiin sisäänrakennetusta tietosuojasta ja tietosuojaperiaatteiden huomioimisesta järjestelmissä ja sovelluksissa. Tietoturvatestauksilla voidaan varmistaa ja osoittaa, että järjestelmien toteutus vastaa suunniteltua ja, että tietoturvaan liittyvät kontrollit on toteutettu oikein (Valtiovarainministeriö 2016). Tietoturvatestaukset ja niistä muodostuva dokumentaatio on keino osoittaa järjestelmien luottamuksellisuus ja eheys.

7 TOIMENPITEIDEN TARKASTUSLISTA

Opinnäytetyössä käsiteltyjen asioiden pohjalta koottiin toimenpiteiden tarkastuslista, jossa kuvaillaan yksinkertaisuudessaan toteutettavat dokumentaatiot ja toimenpiteet, jotka ovat osoitusvelvollisuuden kannalta välttämättömiä. Toimenpiteiden tarkastuslista on liitetty opinnäytetyöhön liitteeksi.

Yksinkertaisuudessaan organisaatioiden tulee dokumentoida henkilötietojen käsittelyn liittyvät toimintatavat, nimetä vastuuhenkilöt, varmistaa käsittelyn lainmukaisuus ja tuottaa henkilöstölle ohjeistuksia sekä kouluttaa henkilöstö tarpeen vaatiessa uusiin toimintatapoihin. Lisäksi organisaatioiden tulee teettää tarvittavat muutokset organisaation järjestelmiin sekä verkkoon, testata muutokset ja luoda riskienhallintaprosessit.

8 POHDINTA

Opinnäytetyön viimeisessä luvussa kuvaan oman työni kautta tulleita omia ajatuksiani osoitusvelvollisuuden täyttymisestä organisaatioissa sekä opinnäytetyön tavoitteiden toteutumisen ja eteen tulleet haasteet.

8.1 Yleisesti

Kuten opinnäytetyö on kuvannut, tuo tietosuoja-asetus mukanaan paljon muutoksia henkilötietojen käsittelyyn. Asetus on kuitenkin osaksi hyvinkin paljon tulkinnanvarainen ja organisaatioiden tulee itse pohtia mitä esimerkiksi tietosuojaperiaatteet niiden kohdalla tarkoittavat ja miten ne on otettava huomioon henkilötietojen käsittelyssä. Omaan työhöni tietosuojan parissa verraten voin todeta, että monilla organisaatioilla tietosuojan hahmottaminen ja toteuttaminen toiminnassaan on vielä hyvin puutteellista, puhumattakaan erilaisista dokumentaatioista ja niiden avulla osoitusvelvollisuuteen vastaamisesta. Organisaatioilla on olemassa hyvin paljon vakiintuneita käytäntöjä toiminnassaan, mutta harvoin niitä on kuitenkaan kuvattu prosesseiksi, joissa henkilötietojen käsittelyn kohdistuvat toimintatavat tulisivat ilmi. Samoin harvoilla organisaatioilla on ollut olemassa henkilöstölle osoitettuja ohjeistuksia, joilla voitaisiin osoittaa henkilöstön tietämys henkilötietojen parissa toimimisesta.

Tietosuojatyö vaatii useinkin paljon työtä ja oman organisaation toimintatapojen tarkastelua. Tietosuoja-asetuksen soveltaminen alkaa toukokuussa ja henkilötietojen käsittelyn tulee silloin olla asetuksen vaatimalla tasolla. Uskon kuitenkin, että tietosuoja-asetuksen vaatimusten toteuttamiseen on varmasti monilla organisaatioilla vielä pitkä tie, minkä vuoksi onkin erityisen tärkeää priorisoida riskiarvion mukaan tarvittavien toimenpiteiden toteutus ja edetä askel askeleelta.

8.2 Tavoitteiden toteutuminen

Opinnäytetyön päätavoitteena oli selkeän kokonaisuuden kuvaaminen niistä toimenpiteistä, joita organisaatioiden tulisi toteuttaa tietosuoja-asetuksen osoitusvelvollisuuden täyttämiseksi. Opinnäytetyön oli valmistuttuaan tarkoitus olla ohjeistustyyppinen kokonaisuus, joita toimeksiantajana toimivan, oman työpaikkani asiakasorganisaatiot voivat käyttää apunaan tietosuojatyössään. Tavoitteessa onnistuttiin, mutta nähtäväksi jää vielä, koetaanko opinnäytetyö organisaatioiden apuna tietosuojatyössä. Myös omalle oppimiselle asetetut tavoitteet toteutuivat, sillä työn edetessä esille tuli paljon uutta ja omaa tietämystä täsmentävää tietoa. Tietosuoja-asetuksen määrittämän osoitusvelvollisuuden hahmottamisesta näin läheltä, miltei ruohonjuuritasolta on varmasti hyötyä tulevaisuudessa omien työtehtävieni parissa.

8.3 Haasteet

Opinnäytetyön kirjoittamisen aikana en kohdannut mielestäni kovinkaan suuria haasteita. Kohtalaiseksi haasteeksi voin kuitenkin todeta muodostuneen aikaisemminkin mainitsemani tietosuoja-asetuksen tulkinnanvaraisuuden. Jotta opinnäytetyön lopputuloksesta sai selkeän ja yksiselitteisen, oli ajoittain hankala kuvata toimenpiteitä mahdollisimman yksinkertaisesti heijastamatta niitä tietyn tyyliseen henkilötietojen käsittelyyn. Kevyenä haasteena koin myös osittain sisällön tuottamisen soveltavassa osuudessa niihin toimenpiteisiin, joista itselläni on vähemmän tietämystä. Lisäksi aiheen tuoreus vaikutti lähteiden valintaan paljon. Luotettavia ja ajan tasalla olevia lähteitä varsinkin kirjallisuudessa oli saatavilla hyvin vähän. Onneksi verkkojulkaisut tukivat työtä kattavasti, mutta niidenkin ajantasaisuutta piti tarkastella tovi, ennen kuin niin sanotusti uskalsi luottaa tiedon pätevyyteen vielä tänä päivänä. Viimeisenä yhdeksi haasteeksi voin myös mainita opinnäytetyön kokonaisuuden rakentamisen. Alusta alkaen minulle oli hyvin selkeää opinnäytetyön lopputulos ja se, mitä työhöni haluan sisällyttää. Matkan varrella työn muoto kuitenkin muuttui useaan kertaan, ja tiedon jäsentely niille sopiville kohdille tuotti välillä hankaluuksia. Monet sisältötekstit saattoivat sopia moneen eri alueeseen, joten oli vaikeaa rajata ja rakentaa työ niin, että se olisi mahdollisimman looginen ja ettei työssä esiintyisi toistoa.

LÄHTEET

Euroopan parlamentin ja neuvoston asetus (EU) 2016/679. Annettu 27.4.2016. Saatavilla http://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX%3A32016R0679

Hanninen, M.; Laine, E.; Rantala, K.; Rusi, M.& Varhela, M. 2017. Henkilötietojen käsittely. Eu-tietosuoja-asetuksen vaatimukset. Vantaa: Kauppakamari

Henkilötietolaki 22.4.1999/523. Annettu Helsingissä 22.4.1999. Saatavilla http://www.finlex.fi/fi/laki/ajantasa/1999/19990523

Koivunen, E. 2011. LIITE 4: Esimerkki Tietoturvapolitiikka (Vahti3/2007). Valtiovarainministeriö. Viitattu 25.3.2018. https://www.vahtiohje.fi/web/guest/602?p_p_id=77&p_p_lifecycle=1&p_p_state=normal

Pietikäinen, S. 2016a. 4 Rekisteröidyn oikeudet. Valtiovarainministeriö. Viitattu 12.2.2018 https://www.vahtiohje.fi/web/guest/rekisteroidyn-oikeudet

Pietikäinen, S. 2016b. Rekisterinpitäjän velvollisuudet. Valtiovarainministeriö. Viitattu 13.2.2018 https://www.vahtiohje.fi/web/guest/rekisterinpitajan-velvollisuudet

Opitietosuojaa.fi 2015. Käyttövaltuusperiaatteet. Viitattu 24.3.2018 https://opitietosuojaa.fi/index.php/fi/aloitus/tietosuojavastaava/49-tyokalupakki/periaatteet-politiikat-ja-suunnitelmat/52-kayttovaltuusperiaatteet

Suomen Automaatioseura ry 2010. Teollisuusautomaation Tietoturva. Viitattu 1.4.2018 https://www.viestintavirasto.fi/attachments/tietoturva/TeollisuusautomaationTietoturva.pdf

Talus A.; Autio E.; Hänninen A.; Pihamaa H-T. & Kantonen S. 2017. Miten valmistautua EU:n tietosuoja-asetukseen? Helsinki: Oikeusministeriö. Saatavilla http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/1Em8rT7IF/Miten_valmistautua_EUn_tietosuoja-asetukseen.pdf.

Tietosuojavaltuutetun toimisto 2015. EU:n tietosuojauudistus. Viitattu 2.2.2018 http://www.tietosuoja.fi/fi/index/euntietosuojauudistus.html#tietosuoja-asetus

Tietosuojavaltuutetun toimisto 2016. Kysymyksiä ja vastauksia tietosuojauudistuksesta. Viitattu 5.2.2018 http://www.tietosuoja.fi/fi/index/euntietosuojauudistus/kysymyksiajavastauksia.html

Tietosuojavaltuutetun toimisto 2014a. Rekisteri- ja tietosuojaselosteet. Viitattu 7.3. 2018 http://www.tietosuoja.fi/fi/index/materiaalia/lomakkeet/rekisteri-jatietosuojaselosteet.html

Tietosuojavaltuutetun toimisto 2014b. Laadi tietotilinpäätös. Viitattu 8.3.2018 http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/tiedotteet/6JEcJrDjj/Laadi_tietotilinpaatos.pdf

Tietosuojavaltuutetun toimisto 2013. Mitä tietosuojalla tarkoitetaan. Viitattu 11.3.2018 http://www.tietosuoja.fi/fi/index/lapsillejanuorille/mitatietosuojallatarkoitetaan.html'

Tietosuojavaltuutetun toimisto 2012. Lokitiedot henkilötietojen suojaamisen välineinä. Viitattu 11.3. 2018 http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/kaytonvalvonnanohjeet/wPJBn9UGn/Kaytonvalvonta_Lokitiedot_henkilotietojen_suojaamisen_valineina_paiv._10.06.2014.pdf

Tietosuojavaltuutetun toimisto 2017. Tietosuojavastaavat. Viitattu 28.3.2018 http://www.tietosuoja.fi/fi/index/euntietosuojauudistus/ohjeitarekisterinpitajalle/tietosuojavastaavat.html

Valtiovarainministeriö 2016. EU-tietosuojan kokonaisuudistus. Viitattu 3.3.2018 https://www.vahtiohje.fi/c/document_library/get_file?uuid=ddb05959-40d1-435f-af23-fd20fc21d63f&groupId=10229

Valtiovarainministeriö 2009. Lokiohje. Viitattu 25.3.2018. https://www.vahtiohje.fi/c/document_library/get_file?uuid=775179cb-6c54-4dfb-b65d-e925d47c61d2&groupId=10229

Vesamäki, P. 2016. [Teema] Vieraskynä: SIEM lokitiedon hyödyntämisessä. Viitattu 26.3.2018 https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2016/03/ttn201603151527.html

Viestintävirasto 2016. Lokien keräys ja käyttö. Viitattu 25.3.2018 https://www.viestintavirasto.fi/attachments/tietoturva/Lokitusohje.pdf

Valtiovarainministeriö 2010. Sisäverkko-ohje. Viitattu 1.4.2018 https://www.vahtiohje.fi/c/document_library/get_file?uuid=5084ce47-32bf-4025-bcc1-73fc2de4edad&groupId=10128

Valtiovarainministeriö 2017a. Tietoturvapoikkeamatilanteiden hallinta. Viitattu 29.3.2018 https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/79258/VM_8_2017.pdf?sequence=6

Valtiovarainministeriö 2017b. Ohje riskienhallintaan. Viitattu 29.3.2018 https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/80013/VM_22_2017.pdf?sequence=1